GOVERNMENT OF INDIA
ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:6308
ANSWERED ON:12.04.2017
Aadhaar Enabled Payment
Roy Prof. Saugata

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

Will the Minister of ELECTRONICS & INFORMATION TECHNOLOGY be pleased to state: -

(a) the status of the Aadhaar-enabled payment authentication in the country, State-wise;

(b) the details of the services available through the system;

(c) the details of business done since its implementation; and

(d) the steps taken to protect the data?

Answer

(a) and (b): Aadhaar Enabled Payment System (AEPS) is owned, operated and maintained by NPCI. AEPS is a bank led model which allows online interoperable financial inclusion transaction at PoS (MicroATM) through the Business Correspondents of any bank using the Aadhaar authentication. Following services are available through AEPS: balance enquiry, cash withdrawal, cash deposit, fund transfer, demographic authentication and e-Know Your customer (e-KYC).Under AEPS resident authentication is done by UIDAI and transaction authentication is done by NPCI and Banks. State-wise data of Aadhaar-enabled payment authentication is not maintained.

(c): The following are the details of business done since its implementation:

Financial Year 2012-13 2013-14 2014-15 2015-16 2016-17
On-us approved Transactions (in Millions) 0.2 11.15 16.37 94.3 319
Off-us approved Transactions (in Millions) 0 0 0.000052 0.74 25.84
Total approved Transactions (in Millions) 0.2 11.15 16.37005 95.04 344.84

(d): All specifications as notified by UIDAI & STQC for biometric devices are adhered to on transaction points. Also, solution handling / addressing multiple aspects of network security, database security, processes and people security are put in place at all the points in the transactions ecosystem i.e at acquirer banks, NPCI and issuer banks. Further, the Reserve Bank of India has issued a comprehensive circular on Cyber Security Framework in Banks on June 2, 2016 covering best practices pertaining to various aspects of cyber security.

****